CIBERSEGUROS, LA MEJOR FORMA DE TRANSFERIR RIESGOS DE ATAQUES INFORMÁTICOS

Franco Ricardo
rfrancomahecha@gmail.com
Universidad Piloto de Colombia

Resumen - En este mundo globalizado, las compañías buscan visibilidad a nivel nacional e internacional a través de diferentes tecnologías de información, logrando apalancar nuevos modelos de negocio de alcance mundial.

Una compañía con visibilidad global aumenta los riesgos de brechas de seguridad y las amenazas se multiplican, por este motivo es necesario realizar una adecuada gestión de riesgos, que sean el punto de partida para el correcto aseguramiento de los activos de información.

Cuando los controles para proteger la información son más costosos que el activo a proteger, es el momento para acudir a un seguro, pero si el activo a proteger es información, ¿a qué seguro puedo acudir?

El presente artículo describe la creciente problemática de los ataques informáticos y la necesidad de contar con productos de responsabilidad cibernética como opción de transferencia del riesgo, relacionado con los efectos financieros de un ataque informático, revisando algunas de las opciones de seguros que, al momento de la redacción del presente artículo, están disponibles en Colombia y en el mundo.

Índice de Términos – Análisis de riesgos, Ciberseguros, Hacking, Seguridad de la información.

I. INTRODUCCIÓN

A medida que la tecnología juega un papel cada vez más importante en las compañías y en sus empleados, los riesgos de la seguridad crecen rápidamente y los negocios deben proteger su información y la de sus clientes.

La información es el activo más importante de toda compañía, y protegerlo es un reto cada vez más difícil de afrontar en un mundo hiperconectado.

En varios países de la región, incluido Colombia se han dado los primeros pasos creando un marco de regulación de la seguridad de la información, así como estableciendo Equipos de Respuesta ante Emergencias Informáticas, tales como el CSIRT-CCIT.

Así como los riesgos en seguridad informática evolucionan constantemente también se requiere establecer controles acordes a la realidad que permitan gestionar estos riesgos de forma que sea aceptable por la compañía.

El lector de este artículo encontrará una descripción de las cifras de ataques en Colombia, así como las leyes que aplican en Colombia para las compañías que resguardan datos personales, así como las opciones de ciberseguros en Colombia y el mundo.

II. MARCO TEÓRICO

En la actualidad casi todas las empresas utilizan tecnología para optimizar sus procesos, según el Departamento Administrativo Nacional de Estadística (DANE) para el año 2014, alrededor del 99% de las empresas hace uso por lo menos un computador [1], Esto indica que se están utilizando tecnologías de la información como herramientas para potenciar ventajas competitivas que se traducen en nuevas ventas y presencia en diferentes ciudades, pero también implica exponerse a nuevos riesgos inherentes a uso de estas tecnologías.

Internet ha facilitado la comunicación entre las personas y ha permitido a las empresas llegar más lejos ofreciendo sus productos o servicios a través de un navegador de forma que cualquier persona pueda hacer compras a través de un celular, una tableta o un computador.

Las amenazas a las que están expuestas las compañías a través de Internet difieren a las amenazas físicas debido a que los hackers cuentan con todo su tiempo disponible para encontrar puntos débiles, atacarlos, comprometer la información de la compañía y desaparecer, prácticamente sin dejar huellas.

A. Estado de la Seguridad en Latinoamérica

ESET, empresa europea fabricante de software de seguridad, en el año 2015 realizó encuestas entre diversas compañías de diferentes sectores para conocer el estado de la seguridad de la información.

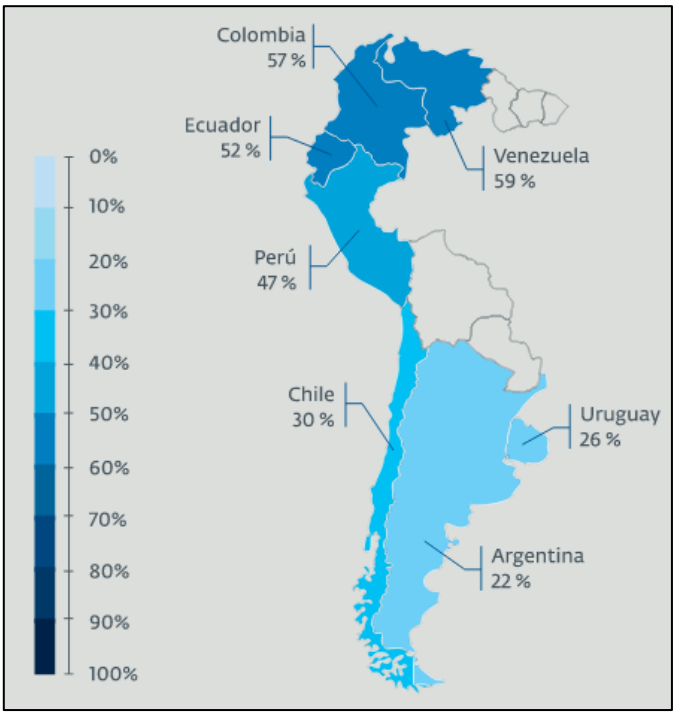

Figura 1: Porcentaje de empresas, por país, que sufrieron un incidente relacionado con infecciones de códigos maliciosos [2]

En la anterior gráfica se muestra que el 57% de las empresas colombianas encuestadas reportan infecciones por malware.

Según Panda Security, en el año 2015, Colombia registró una tasa de infección del 33,17%, por debajo de la media global. [3]

Los códigos maliciosos tipo *Botnet* son una de las amenazas más utilizadas por los cibercriminales ya que *"utilizan virus troyanos especiales para crear una brecha en la seguridad de los computadores de varios usuarios, tomar el control de cada computador y organizar todos los equipos en una red de bots que el cibrecriminal puede gestionar de forma remota."* [4]

Estas redes tipo *Botnet* son usadas frecuentemente para realizar Ataques de Denegación de Servicio (DoS, DDoS), donde todos los equipos infectados generan peticiones al servidor objetivo produciendo un bloqueo en el mismo.

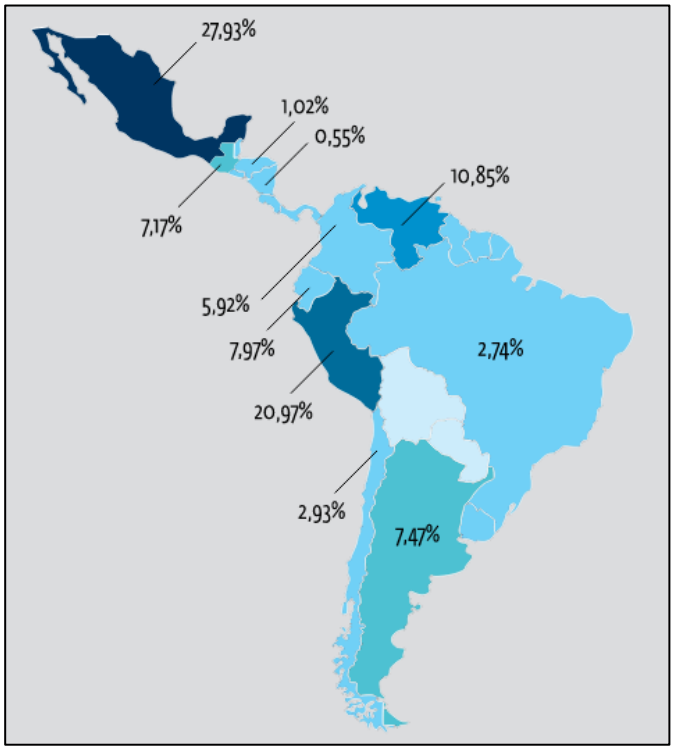

Figura 2: Porcentaje de Bots por país [5]

En la anterior gráfica muestra el nivel de detecciones de código malicioso tipo *bot* en Latinoamérica, se puede observar que Colombia es el sexto país en detección de esta amenaza con un 5,92%.

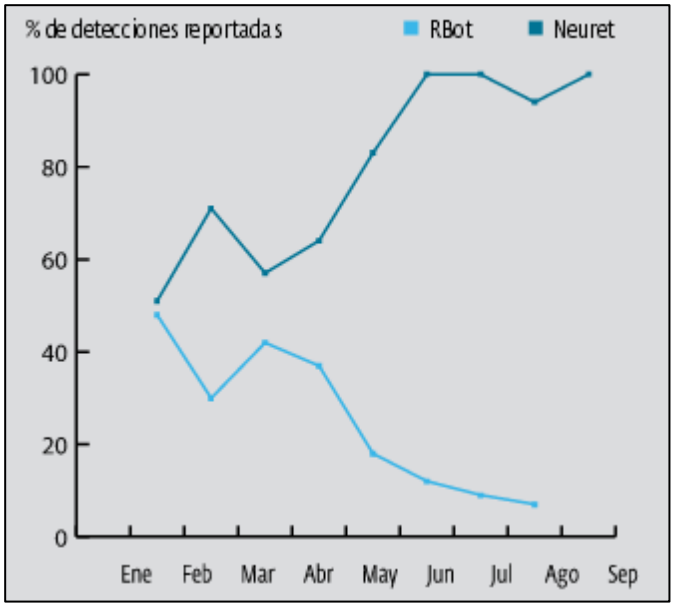

Figura 3: Porcentaje de detección de las amenazas Neuvret vs RBot en Colombia [5]

En el anterior gráfico se comparan dos familias de código malicioso tipo *Botnet* y la cantidad de detecciones en Colombia de enero a septiembre de 2014. Este tipo de código malicioso es una amenaza real para las compañías y es necesario aplicar controles para evitar ser víctima de los ciberdelincuentes.

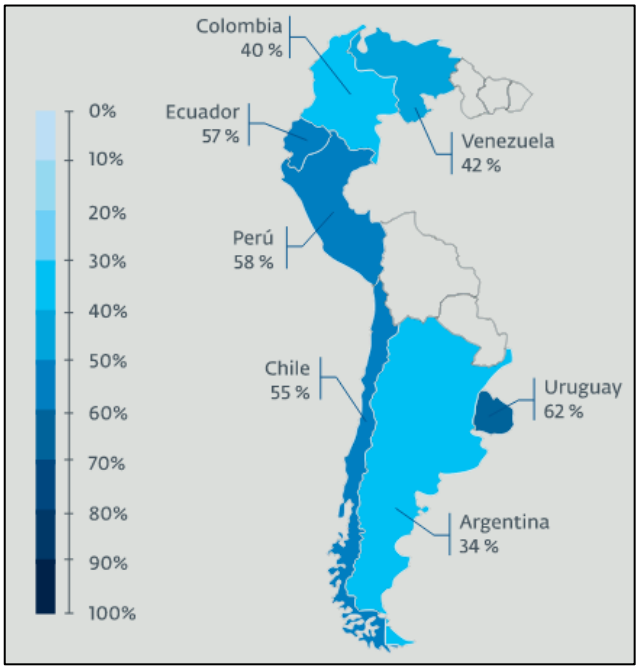

Figura 4: Porcentaje de empresas, por país, que sufrieron un incidente relacionado con acceso indebido a aplicaciones y/o bases de datos [2]

En la anterior gráfica se muestra que el 40% de las empresas colombianas encuestadas reportan accesos indebidos a la información. Esto supone un enorme riesgo para las compañías, especialmente si se trata de datos personales ya que puede tener implicaciones legales que podrían afectar la imagen de la compañía.

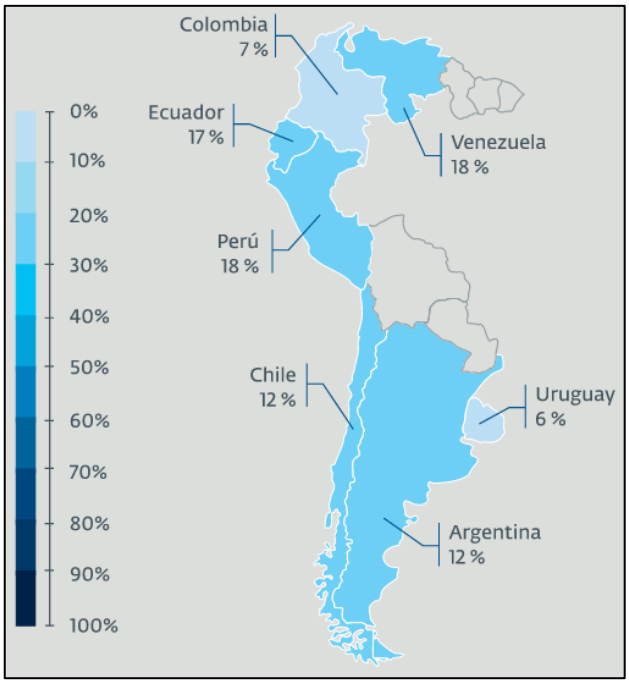

Figura 5: Porcentaje de empresas, por país, que sufrieron un incidente relacionado con explotación de vulnerabilidades [2]

En la anterior gráfica se muestra que solo el 7% de las empresas colombianas encuestadas dicen haber sufrido incidentes relacionados con explotación de vulnerabilidades, esta situación no es sorpresiva, ya que constantemente se publican exploits de las vulnerabilidades de diferentes tipos de software incluso se pueden hallar manuales y videos acerca de cómo utilizarlos.

Según Kaspersky "En el 2015, alrededor de 100 compañías financieras fueron atacadas alrededor del mundo, con pérdidas alrededor de un billón de dólares." [6]

En Colombia la situación no es más alentadora, Según el periódico El Tiempo "*en 2015, cibercrimen generó pérdidas por US$600 millones en Colombia"* [7] este valor está basado en el tiempo que las compañías dejaron de prestar su servicio.

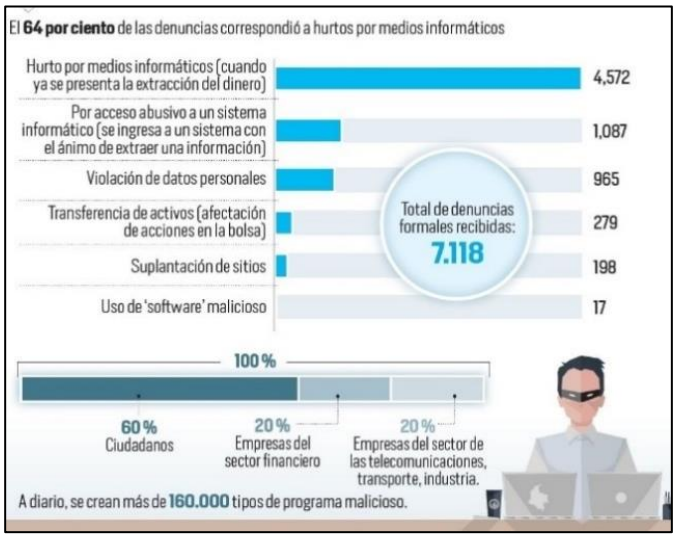

Figura 6: Radiografía de los delitos Informáticos en Colombia en 2015 [7]

Según la revista dinero con un total de 6'600.000 ataques informáticos, el sector más afectado fue el financiero, seguido por el sector gobierno, comunicaciones, energía, industria y comercio. [8]

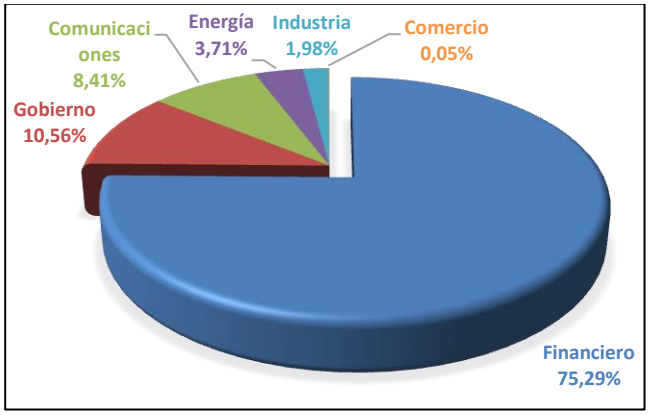

Figura 7: Porcentaje de empresas atacadas por sector Fuente: El autor, 2016

El sector financiero, gobierno y comunicaciones tienen una característica en común: almacenan grandes cantidades de datos personales en bases de datos que son un gran atractivo para los ciberdelincuentes. El robo de este tipo de información significa un enorme riesgo con implicaciones legales y financieras.

De los anteriores datos se podría inferir que las empresas no han invertido suficientemente en controles para contener ataques informáticos, pero en la encuesta realizada por ESET, se muestra que las compañías cuentan con diferentes tipos de controles implementados, aunque se hace notoria la falta de controles para la seguridad en móviles, soluciones de doble autenticación, tecnologías de cifrado y herramientas de detección de intrusos (IDS), como se muestra en la siguiente figura:

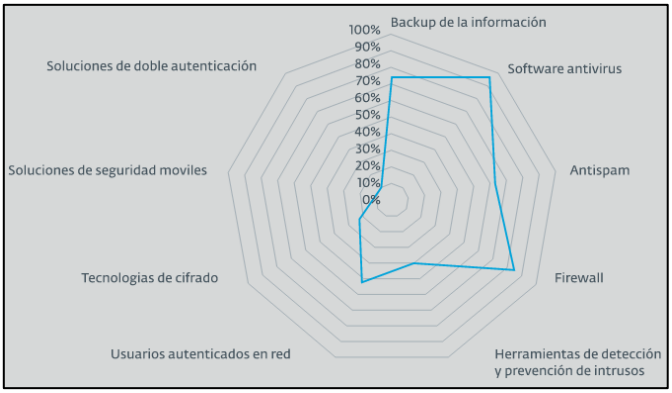

Figura 8: Porcentaje de empresas encuestadas en Latinoamérica que tienen implementados controles basados en tecnología [2]

B. Nuevas tendencias, nuevas amenazas

INTERNET DE LAS COSAS (IoT)

Internet ha cambiado a las personas y su forma de comunicarse, ha cambiado la forma de buscar información y ha logrado masificar el conocimiento, llegando a zonas donde antes era imposible. Estos cambios han dado paso a un sinnúmero de avances tecnológicos que intentan aprovechar las ventajas que las redes de comunicaciones pueden traer a las personas, acá es donde nace el Internet de las Cosas, IoT por sus siglas en inglés.

Y con la evolución de Internet, los dispositivos cotidianos se transformaron en nuevas fábricas de información online.

Esta tendencia de conectar a Internet, televisores, neveras, consolas de videojuegos, equipos de sonido, automóviles, relojes, sensores, cámaras de seguridad, entre otros, supone un conjunto de retos nuevos referentes a la protección de datos personales y la privacidad de los consumidores de estos productos.

"Todas las posibles debilidades que pueden afligir los sistemas IoT, tales como autenticación y cifrado de tráfico, son bien conocidos por la industria de la seguridad." [12]

TRAIGA SU PROPIO DISPOSITIVO (BYOD)

Más que una tendencia, se está convirtiendo en una práctica empresarial aceptada, donde los empleados utilizan dispositivos personales en ambientes laborales, desde teléfonos hasta computadores, prestan servicios personales y corporativos, desde cualquier lugar, promoviendo el teletrabajo, que al final se traduce en una mejora en la calidad de vida del trabajador y en la movilidad de las ciudades.

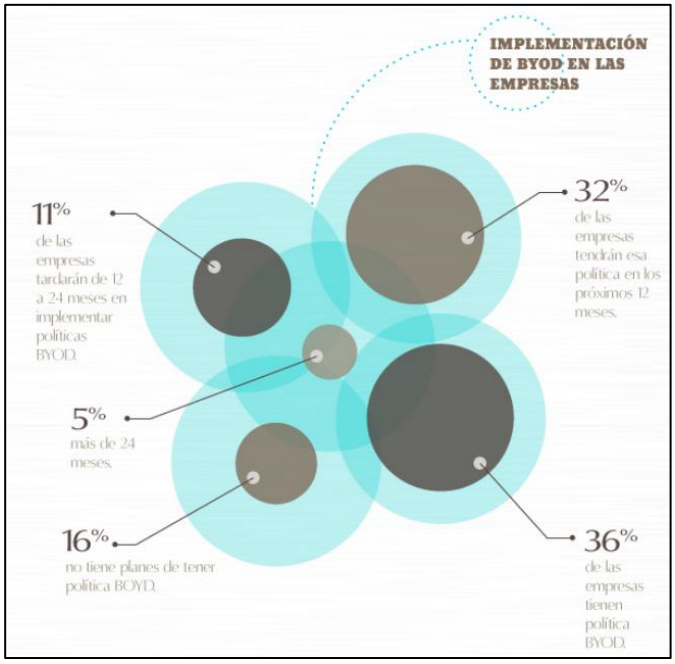

Figura 9: Datos de uso de BYOD en el mundo [13]

C. Entidades de Atención de Incidentes Informáticos en Colombia

En caso de ocurrencia de un ataque informático, las compañías deben acudir a las organizaciones de reacción ante ataques informáticos. Las cuáles serán descritas a continuación:

- Centro de coordinación de seguridad informática Colombia (CSIRT-CCIT)
    - Está en contacto directo con los centros de seguridad de sus empresas afiliadas.
    - Tiene la capacidad de coordinar el tratamiento y solución de incidentes de seguridad informática.
    - Mantiene comunicación constante con organizaciones internacionales que puedan proveer información acerca de contenido malicioso que pueda afectar la seguridad de los afiliados. [9]

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)

Esta entidad es responsable de la coordinación de la ciberseguridad y ciberdefensa nacional, enmarcada dentro del proceso misional de gestión de la seguridad y defensa del Ministerio de Defensa Nacional. Dentro de sus objetivos están:

- Coordinar y asesorar entidades públicas y privadas para responder ante incidentes informáticos.
- Actúa como punto de contacto internacional con sus homólogos de otros países.
- Desarrollar y promover procedimientos, protocolos, guías de buenas prácticas y recomendaciones de seguridad informática.
- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad. [10]

- Centro Cibernético Policial CSIRT PONAL
  Este es el equipo de respuesta a incidentes de seguridad informática de la Policía nacional de Colombia. Dentro de sus servicios esta:

  - Publicar reportes sobre delitos informáticos.
  - CAI virtual – iniciativa de atención policial en línea.
  - Publicar de recomendaciones, boletines, guías, informes e infografías de ciberseguridad.
  - Divulgar información acerca de aplicaciones móviles para el fortalecimiento de la ciberseguridad.
  - Sensibilizar a la comunidad sobre las diferentes modalidades delictivas presentadas por los ciberdelincuentes.
  - Publicar en tiempo real los incidentes informáticos que afectan la ciberseguridad nacional. [11]

D. Legislación

En Colombia hay legislación vigente mediante la cual se dictan disposiciones claras, respecto al tratamiento de datos personales, esta regulación es de obligatorio cumplimiento por toda empresa que opere en territorio colombiano. Entre las más relevantes están:

CONSTITUCIÓN POLÍTICA DE COLOMBIA DE 1991

ARTÍCULO 15: "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.*

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley." [14]

LEY ESTATUTARIA 1581 DE 2012

ARTÍCULO 1: "*La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.*" [15]

ARTÍCULO 5. Datos Sensibles: *"Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos."* [15]

E. Normas Internacionales

Los riesgos relacionados con la seguridad de la información deben ser identificados y gestionados de forma que se disminuya la incertidumbre y se minimicen las pérdidas hasta un punto aceptable.

Es importante para las compañías cuantificar el impacto de la materialización que estos riesgos pueden traer a la compañía (en su imagen y financiero) y las opciones para tratarlos.

La norma internacional ISO 31000:2009 proporciona principios un marco y un conjunto de procesos para la gestión de riesgos, ayudando a las organizaciones con el análisis y evaluación de los mismos, aumentando la fiabilidad del sistema de gestión de la compañía.

Dentro de los procesos establecidos por la norma se describe el tratamiento de riesgos con cuatro opciones principales que serán aplicadas hasta que el riesgo residual sea aceptable por la organización, estas son:

- Reducir el riesgo: Se implementan controles de forma que el nivel de riesgo residual sea aceptable por la compañía.
- Aceptar el riesgo: Se aplica cuando el nivel del riesgo cumple con los criterios de aceptación de la compañía y no es necesario aplicar controles adicionales.
- Evitar el riesgo: Cuando el nivel de riesgo se considera muy alto y el tratamiento del riesgo resulta más costoso que los beneficios, se debe replantear la actividad o la forma en que la actividad es operada.
- Transferir el riesgo: El riesgo es transferido a un tercero que pueda gestionarlo de forma efectiva.

Esta última opción para el tratamiento del riesgo es el tema principal de este artículo ya que la forma más común de transferir el riesgo de los ciberataques es a través de seguros y este es un producto que lleva varios años en el mercado.

III. ALTERNATIVAS DE CIBERSEGUROS

A. Ciberseguros en Colombia

En Colombia solo hay una aseguradora que ofrece un producto especialmente dirigido a compañías que desean hacer frente a los riesgos relacionados a los activos de la información.

La compañía Norteamericana American International Group (AIG), ofrece el producto CyberEdge y objeto de este ciberseguro es:

- Responsabilidad por uso y tratamiento de información:
  - Perjuicios y gastos de defensa relacionada con una violación de datos personales o corporativos.
- Responsabilidad por la seguridad de datos: Perjuicios y gastos de defensa asociados con:
  - Contaminación de datos de terceros por un virus.
  - Denegación inadecuada o errónea de los derechos de acceso a los datos a un tercero asegurado.
  - Hurto de un código de acceso de las instalaciones de la empresa, un sistema informático o de empleados.
  - Destrucción, modificación, corrupción, daño o eliminación de datos almacenados en cualquier sistema informático.
  - Hurto de hardware de la empresa, que contenga datos personales o corporativos.
  - Revelación de datos como consecuencia de una violación a la seguridad de datos. [15]

El alcance de este seguro busca proteger a la compañía de las consecuencias legales provocadas por una intrusión en los sistemas informáticos de una empresa.

B. Ciberseguros en el Mundo

La compañía alemana Allianz cuenta con un producto llamado Cyber Protect y su cubrimiento está disponible en Europa, Asia y Canadá; Su alcance es:

- Responsabilidad por violación de datos, personales y corporativos.
- Costos por violación de datos, incluye costos de notificación y costos de Tecnologías Informáticas Forenses.
- Responsabilidad por la seguridad de red – para sistemas hackeados o comprometidos incluyendo ataques de denegación de servicios.
- Responsabilidad de medios – para publicaciones digitales.
- Interrupción del negocio – causado por un ciberincidente.
- Costos de restauración para programas y datos – resultado de un ciberevento que interrumpa el negocio.
- Comunicación de crisis – para mitigar el daño a la reputación.
- Seguro de robo por hackers – basado en el robo de fondos.
- Responsabilidad por pagos electrónicos – Cubrimiento por multas y sanciones PCI (Payment Card Industry). [16]

Las compañías británicas ABI y Hiscox cuentan con los productos Cyber Insurance y Cyber and data risk insurance respectivamente, y su cubrimiento incluye:

- Pérdida o daño de activos digitales tales como data o programas de software.
- Interrupción del negocio por inactividad de red.
- Ciberextorsión donde terceros pueden dañar o dar a conocer información si no se les paga algún dinero.
- Gastos de notificación a los clientes cuando hay un requisito legal o regulatorio en caso de una violación de seguridad o privacidad.
- Daño a la reputación derivado de una violación de datos que resulten en la pérdida de propiedad intelectual o clientes.
- Robo de dinero o activos digitales a través del robo de equipos o robo electrónico.
- Violaciones de seguridad y privacidad, la investigación, gatos de defensa y reparación civil asociados con ellos.
- Responsabilidad multimedia, para cubrir la investigación, gastos de defensa y daños civiles derivados de la difamación, violación de la

privacidad o negligencia en la publicación en medios electrónicos o impresos.
- Pérdida de datos de terceros, incluyendo el pago de indemnizaciones a los clientes por denegación de servicios y falla de software o sistemas.

IV. CONCLUSIONES

- Las empresas colombianas han avanzado en temas de seguridad informática respecto a otros países de Latinoamérica, pero es necesario tomar medidas para disminuir la incidencia de los ataques informáticos en el país.
- Con el creciente uso de dispositivos móviles, es importante reforzar los controles de seguridad informática para contener posibles ataques.
- En Colombia solo existe una opción de Ciberseguro, lo que indica que no hay suficiente mercado para plantear competencia o no esta en la cultura colombiana adquirir seguros para gestionar los riesgos informáticos.
- Las pólizas de responsabilidad cibernética son una solución para transferir el riesgo de un ataque informático a un tercero que se encargue de asumir las consecuencias legales del mismo.
- Esta solución de seguros puede asumir los costos legales que se desprendan de una demanda relacionada con datos personales comprometidos, pero no puede solucionar una imagen corporativa debilitada por un ataque informático.

V. REFERENCIAS

[1] Departamento Administrativo Nacional de Estadistica (DANE), «Comunicado de prensa,» 28 diciembre 2015. [En línea]. Available: http://www.dane.gov.co/files/investigaciones/boletines/tic/cp_tic_empresas_2014.pdf. [Último acceso: 12 marzo 2016].

[2] ESET, «ESET Security Report Latinoamérica 2015,» 2015. [En línea]. Available: http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf. [Último acceso: 27 Marzo 2016].

[3] PANDA SECURITY, «27% of all recorded malware appeared in 2015,» 25 Enero 2016. [En línea]. Available: http://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/. [Último acceso: 27 Marzo 2016].

[4] Kaspersky Lab., «¿Qué es un botnet?,» Kaspersky Lab., 2016. [En línea]. Available: www.kaspersky.es/internet-security-center/threats/botnet-attacks. [Último acceso: 3 abril 2016].

[5] ESET, «Tendencias 2015 El mundo corporativo en la mira,» 2015. [En línea]. Available: http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_2015_eset_mundo_corporativo.pdf. [Último acceso: 3 abril 2016].

[6] M. Gaernaeva, J. Van der Wiel, D. Makrushin, A. Ivanov y Y. Namestnikov, «Kaspersky Security bulletin,» 15 diciembre 2015. [En línea]. Available: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. [Último acceso: 12 marzo 2016].

[7] EL TIEMPO, «En 2015, cibercrimen generó pérdidas por US$600 millones en Colombia,» 28 enero 2016. [En línea]. Available: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604. [Último acceso: 12 marzo 2016].

[8] Revista Dinero, «El cibercrimen es un delito más rentable que el narcotráfico,» Revista Dinero, 28 septiembre 2015. [En línea]. Available: http://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988. [Último acceso: 2016 abril 9].

[9] CSIRT-CCIT, «Centro de Coordinación SeguridadInformática Colombia CSIRT-CCIT,» 2016. [En línea]. Available: http://www.csirt-ccit.org.co/nosotros.html. [Último acceso: 11 Abril 2016].

[10] colCERT, «Grupo de Respuesta a Emergencias Cibernéticas de Colombia colCERT,» 8 julio 2013. [En línea]. Available: http://www.colcert.gov.co/?q=acerca-de. [Último acceso: 11 abril 2016].

[11] Ministerio de Defensa Nacional - Policía Nacional de Colombia, «Centro Cibernético Policial,» 2016. [En línea]. Available: http://www.ccp.gov.co/#servicios. [Último acceso: 11 abril 2016].

[12] M. Ballano Barcena, «Insecurity in the Internet of Things,» Marzo 2015. [En línea]. Available: https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf. [Último acceso: 6 abril 2016].

[13] Ixotype, «BYOD en España,» Ixotype, 2013. [En línea]. Available: http://www.ixotype.com/media/byod_infografia_ixotype..jpg. [Último acceso: 9 abril 2016].

[14] Alcaldía Mayor de Bogotá, «Constitución Política de Colombia,» 1991. [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125#15. [Último acceso: 28 marzo 2016].

[15] Alcaldía Mayor de Bogotá, «Constitución Política de Colombia,» 1991. [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Último acceso: 14 abril 2016].

[16] AIG, «CyberEdge,» 2016. [En línea]. Available: https://www.aig.com.co/empresas/nuestros-productos-empresas/lineas-financieras/cyberedge. [Último acceso: 26 marzo 2016].

[17] Allianz, «Allianz Cyber Protect,» 2015. [En línea]. Available: http://www.agcs.allianz.com/services/financial-lines/cyber-insurance/. [Último acceso: 30 marzo 2016].

[18] E. Medina, «En 2015, cibercrimen generó pérdidas por US$600 millones en Colombia,» 28 enero 2016. [En línea]. Available: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604. [Último acceso: 12 marzo 2016].

Franco, Ricardo. Nació en Bogotá en 1982. Recibió el título en Ingeniería de Sistemas de la Universidad Católica de Colombia, Bogotá D.C., en 2011. Actualmente está optando al grado de Especialista en Seguridad Informática en la Universidad Piloto de Colombia.